(2)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 November 2000 (30.11.2000)

PCT

(10) International Publication Number
WO 00/72171 A1

(51) International Patent Classification⁷: G06F 15/177

(21) International Application Number: PCT/US00/14279

(22) International Filing Date: 24 May 2000 (24.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/135,790 24 May 1999 (24.05.1999) US
11/863,101 24 May 2000 (24.05.2000) US

(71) Applicant and
(72) Inventor: PERRY, Gregory [US/US]; 7828 Flager Circle, Manassas, VA 20109 (US).

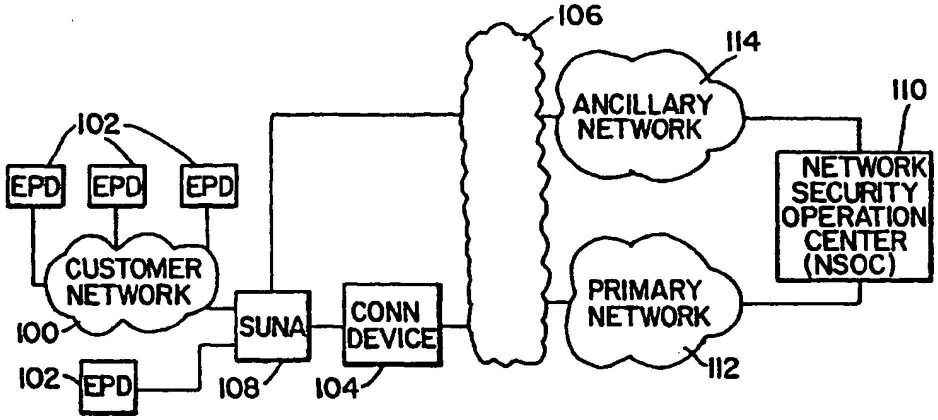
(74) Agent: STEIN, Laurence, E.; Patton Boggs LLP, 2550 M Street, N.W., Washington, DC 20037 (US).

(84) Designated States (*regional*): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR REMOTELY MANAGED LOCAL NETWORK INTERFACE SECURITY



(57) Abstract: A remotely configurable transmission security filtering, monitoring and alarm unit (108) is installed locally between an end-user's workstation (102) or network (100) and a wide-area, non-secure network (106) like the Internet. A management unit (104) for configuring and monitoring one or more of the remotely configurable security units (108) connects to the wide-area network (106) and transfers alarm criteria and other configuration data particular to each security unit (108). The local security units (108) filter digital transmissions between their workstations (102) or network (100) and the wide-area network (106) such as the Internet, according to the alarm criteria. The management unit (110) may upload encryption parameters to the remote local security units (108). In response to new security information, such as newly discovered security threats, the management unit (104) reconfigures the alarm criteria at the local security units at their respective locations around the Internet or other wide-area network (106).

WO 00/72171 A1

METHOD AND APPARATUS FOR REMOTELY MANAGED LOCAL NETWORK INTERFACE SECURITY

DESCRIPTION

Field of the Invention

This invention relates generally to the field of network security and, more particularly, to remote configuration, management and monitoring of message traffic between local area networks and wide-area non-secure networks such as the Internet.

Description of the Related Art

The number of consumers and businesses using telecommunication for exchanging information and conducting business continues to increase. One technological field showing a particularly large increase in use is the Internet, both by consumers and by business of all sizes, from one-person operations without "brick and mortar" establishments, to large companies such as IBM, General Motors, and Microsoft. The Internet is used for exchange of data representing almost every level of conducting business, from interaction between consumers, business-to-business interaction, and interaction between businesses and consumers. The Internet is also used for inter-office exchanges within geographically distributed companies, and by companies utilizing off-site and out-sourced accounting and other data management services.

The Internet continues to evolve into a vast, highly connected, very high capacity network connecting virtually any computer, anywhere in the world, having the required interface capacity with any other computer, network of computers, database servers, and other sources of digital or digitized information. The Internet, however, is not a secure transmission media. Indeed, as is well known to one of ordinary skill in the art, the very complexity of the Internet has and continues to create ever-increasing opportunities for unauthorized access to, or interruption of, computer resources and data transmissions. These range from amateur acts to well-directed expert attacks from the outside into a company's internal network, exploiting the network's portal to the Internet and utilizing the newest "hacking" methods. These acts are disruptive, intrusive and costly.

There are various known preventative measures for countering these attacks. One is method is to construct or implement what is termed a "firewall" between the company's internal or local area network (LAN) and the Internet.

Various configurations of firewalls are known in the art, but most subject traffic between the Internet and the LAN to a filtering operation, on a packet-by-packet basis. The filtering is generally referred to as "packet filtering." Based on what the packet filtering detects the packet is blocked, blocked and stored for manual inspection, passed through with a notice sent to the system administrator, or passed through without further action. Packet filtering can be simple, such as inspecting certain header fields of, for example, TCP/IP formatted packets, or can be more sophisticated, detecting specific source address features or instruction sequences within executable code.

A difficulty with packet filters arises in selecting and updating the filter rules or criteria. Typically the rule selection is done by the network administrator. However, this can be an ongoing and time consuming task, as it requires the network administrator to keep abreast of the latest security threats and risks, as well as the latest offerings from the network security vendors, in addition to updating the packet filter rules to accommodate the same. Further, the network administrator must take the time to test and troubleshoot the updates. Still, further, the testing introduces another uncertainty, as the set of test vectors selected by the network administrator may not duplicate the real word security threat adequately to locate some faults with the packet filtering program.

Due in part to the issues identified above, in the real business world many network administrators cannot devote the necessary time to such matters. In addition, many businesses cannot afford the continual training that such an administration task requires. The result is that many networks do not have their firewall packet filters updated often enough to block the newest virus attacks or thwart the latest hacker methodologies.

In addition to the security issues arising from data packets received from the Internet, many business use firewalls to filter packets exiting their LAN onto the Internet. The filtering is employed to detect and block employees from inadvertently or intentionally transmitting sensitive data, without the necessary approval or without proper encryption. Encryption is frequently necessary for geographically distributed companies that must communicate sensitive information from the LAN at one of its locations to the LAN at another of its locations.

Techniques for dealing with some of the general network security issues are documented in various publications, including those found in the United States Patent and Trademark Office (USPTO). One example is the intrusion detection disclosed by U.S. Patent No. 5,557,742. Another example is the intrusion detection disclosed by U.S. Patent No. 5,881,225, and U.S. Patent No. 5,774,650. Still another example is the firewall method and apparatus disclosed by U.S. Patent No. 5,826,014. Other examples include secure transmission and cryptography, as disclosed by U.S. Patent Nos. 4,227,253, 4,918,728, 5,864,667 and 5,872,846.

Development of these and other known network security methods and apparatus have been primarily driven by needs for secure financial transactions occurring via the Internet. These technologies have also found use in larger corporate telecommunications systems, especially in systems carrying transaction data between the corporate entity and the United States government.

None of these, however, directly address the problem of requiring network system administrators to maintain the security apparatus and software monitoring and filtering communications between their networks or workstations and the Internet.

More particularly, architectures for the existing methods are usually built upon existing workstations and servers. Companies such as UUNet®, the Sun/Cisco/Pilot joint venture, and services such as those offered by Technologic/Avdata target corporate clients with very sophisticated services for security and VPN tunneling. But in each case, integration into the end user site requires significant time, personnel and hardware, which is very cost prohibitive for smaller organizations or home users. In the case of remote appliances such solutions may be too costly to justify, using conventional cost/risk analysis. As a result, many remote sites still use dedicated networks for lack of an inexpensive, monitored, secure network appliance that could utilize unsecured public networks such at the Internet.

In addition to cost, operation of these commercial systems requires technical ability which is frequently not available to smaller offices. Devices such as the SonicWall™, offered by Sonic Systems™, and software suites, which are pared down commercial packages, are becoming available at the consumer level for use by small office and home users. However, according to a recent installment of "Security Watch" in the January 25, 1999 issue of the periodical Info World, "most will resist the idea of complex firewall technology standing between them and the Internet."

The present inventor has identified, based on the information identified and studies above, that a method for delivering services for security and connectivity enhancement at the level of the regular home user and small business is bother widely desired and required. However, the present inventor has also identified, as been stated in numerous publications, that many people continue to feel intimidated with computer technology and, as such, are self-proclaimed "technophobes." The present inventor has found this to be apparent from various publications, including that of U.S. Patent No. 5,875,108, which states "Significant difficulties are experienced by users when complex programmable devices having multiple commands which are infrequently used or programmed by those users."

In addition, as stated above, end users may not exhibit timeliness in maintaining the system software - even when notified that newer code is available. Even further, in the case of remote sites with appliance-based equipment devices, such as the SonicWall and other stand-alone, user configured equipment can be difficult to install and maintain.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a system and apparatus for secure communication between a local area network (LAN) and a larger wide area network (WAN), such as the Internet, having connectivity enhancement, and having its configuration, programming, monitoring and control performed from a remote location, and being totally transparent to the end user and easily integrated into existing connectivity devices and telecommunication providers' services.

It is a further object of the invention to provide outsourced management of communication security and connectivity between a LAN and the Internet or other WAN, thereby relieving the LAN operator from the time and cost of maintaining updated security capability.

A still further object of the invention is to provide an apparatus and method for immediate updating of one or more LANs' or remote Internet-accessible sites' respective interfaces to the Internet from one or more central locations remote the LANs, thereby providing Internet-wide updating of security capability. The centrally managed updating operation could be in response to detection at any part of the Internet of a new security threat requiring updated filter and detection parameters at each local Internet interface.

Yet another object of the invention is provide a system and apparatus for performing encryption locally at one or more LANs' respective interface to the Internet, with configuration and updating of the encryption being managed from a central facility.

Also, other features such as newer encryption techniques and service to enhance network connectivity are able to be applied without the need for any end user intervention or as in a remote system, any service calls.

One embodiment of the invention is a method for controlling traffic between a first network, such as a corporate LAN, and a second network, such as the Internet, comprising steps of:

connecting an interface unit between the first and the second network, said interface unit having a processor and a data storage unit;

providing a management unit remote from the first network, the management unit having means for receiving criteria selection commands and means for transmitting alarm criteria commands, based on the criteria selection commands, to the interface unit over a management communication network;

providing the management communication network;

transferring the alarm criteria from the management unit to the interface unit over the management communication network;

storing the alarm criteria in the data storage unit;

receiving, at the interface unit, a digital communication between the first network and the second network;

comparing a content of the digital transmission to the alarm criteria, the comparing performed by the data processor; and

generating an alarm from the interface unit based on the comparing.

For consistency in reference labels used in this description, the interface unit of the invention that is local to the user and which performs the described monitoring, filtering and alarm functions will be referenced hereinafter as the "Secure Universal Network Appliance", or "SUNA".

A further embodiment of the invention is a method according to the first embodiment further comprising a step of blocking the digital transmission from being communicated between the first network and the second network based on the comparing.

A still further embodiment is a method according to the first or second embodiment further comprising steps of:

providing an encryption unit with the SUNA,

loading an encryption algorithm into the encryption unit; and

selectively encrypting a digital communication from the first network to the second network, according to the encryption algorithm, based on a result of the comparing step.

A still further embodiment of the invention is a method according to any of the above embodiments which utilizes the second network as the management communication network.

Yet another embodiment of the invention is a method according to any of the above embodiments, further comprising a step of providing an ancillary management communication between the management control unit and the SUNA.

The method and apparatus of the present invention is not solely based on a single device or software. Instead the invention comprises a system having a central security management unit and the SUNA, the SUNA being inserted between a user's LAN or a user's remote site, and a WAN, such as the Internet, with which the LAN or remote site communicates. The central security unit can be maintained and operated by specially trained and experienced computer security professionals independent from, and not requiring management and training by the user. It is envisioned that professionals in the field of computer security, due to having specialized training access to information not widely disseminated, in addition to being not burdened with day-to-day system administration tasks, can be better informed as to up-to-the-minute security issues. This includes keeping up to date as to the identity or and methods employed by those that perpetrate telecommunication ("phreaking"), computer/internet-based ("hacking") intrusions and exploitations.

The present invention, by providing centralized configuration and management of the network interface security operations of businesses and individual users, and thus providing centralized, dedicated intelligence gathering and countermeasure development, allows the system described to stay abreast of the latest techniques and enact defenses at all locations.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects, and advantages will be better understood from the following description of preferred embodiments of the invention with reference to the drawings, in which:

Fig. 1 is a block diagram of an example system according to the invention;

Fig. 2 is a high level circuit diagram of a remotely configurable network security appliance within the example system of Fig. 1;

Fig. 3 is a high level circuit diagram of an alternative configurable network security appliance within the example system of Fig. 1;

Fig. 4 is a system diagram of an example embodiment of the invention, utilizing a remotely configurable network security appliance according to Fig. 3; and

Fig. 5 is a system diagram of an example embodiment of the invention, utilizing a remotely configurable network security appliance an appliance according to Fig. 2.

DETAILED DESCRIPTION OF THE INVENTION

The system and method of this invention will be described with reference to Figs. 1-5 herein.

Fig. 1 depicts a high level system diagram of an example embodiment of the invention. The system comprises a customer network or LAN 100 which may, for example, be an Ethernet bus connecting a plurality of workstations, or standalone user end point devices 102. The LAN 100 includes a server (not labeled) which may be one of the workstations 102. The system further comprises a telecommunication provider's network connection device, or TPIC, 104 which connects to the Internet or other wide area network(WAN) 106. Inserted between the customer network 100 and the TPIC 104 is a Secure Universal Network Appliance or SUNA 108 which, as will be described hereinbelow, performs packet filtering and encryption operations on telecommunication transfers between the in accordance with a remotely loaded configuration, as will also be described.

The example system of Fig. 1 further includes a standalone workstation 102 connected directly to the SUNA 108, which is optional and shown for purposes of example only. The system further includes a Network Security Operation Center, or NSOC, 110 which, as will be described, transfers filtering and encryption commands to the SUNA 108. In the Fig. 1 example system, the NSOC 110 is connected to the wide area network 106, such as the Internet, by a primary network 112, and a back-up, or ancillary network 114. The primary network can, for example be commercial Internet Services Provider (ISP), such as America On Line®. The ancillary network 114, which may be another ISP, is not required but is preferred, in view of the general fault tolerance requirements for security systems.

An example of the SUNA unit 108 will be described in reference to Figs. 2 and 3, with Fig. 1 being a first level functional breakdown of an example SUNA 108, and Fig. 3 depicting an example lower level breakdown of the Fig. 2 embodiment.

The high level block diagram of Fig. 2 depicts the major functional components of an example SUNA apparatus 108 according to this invention. As shown, a high speed central processing unit (CPU) 202A connects to an input/output (I/O) processor 207. CPU 202A and I/O processor 207 are shown as separate units for purposes of describing the operation of the SUNA unit. One contemplated hardware example implements the CPU 202 and I/O processor 207 on a monolithic central processing unit 202A, as shown in the detailed depiction of the SUNA 108 shown at Fig. 3. The combined implementation of these functions 202 and 207 on a single chip is well known in the art.

Referring to Fig. 2, a memory subsystem 209, which includes volatile, non-volatile and mass storage devices (not shown), is multiply ported to the CPU 202, and to the I/O processor 207, a crypto-engine 208 and a digital signal processing (DSP) cluster 203. The multiple port connection allows any of the sub-systems 202, 203 and 208 access to data files, and permits communication between the subsystems as well. The multiple port connection also reduces bottlenecking. Multiple media interfaces 206 provide connection to any of the commonly used network protocols and physical media by way of the I/O processor 207. The network protocols and include Asynchronous Transfer Mode (ATM), Ethernet 100/10bt, and any other network interfacing found in the commercial and consumer environments. The only limitation as to network protocol and physical media is imposed by the system speed. Currently, speeds in excess of OC3 and approaching OC12 are possible.

As described, the example SUNA 108 of Fig. 2 includes a crypto-engine 208. As will be described below, the crypto-engine 208 performs on-demand enciphering and deciphering of communications passed between any of the desired media interfaces 206 via the I/O processor 207 into the crypto-engine 208. There are a plurality of alternative embodiments, or options, within any given embodiment for loading the encryption control software (not shown) into the crypto-engine 208. One alternative is to load the crypto-engine 208 such as, for example, by way of the CPU subsystem 202 during manufacture or during installation. Another alternative is to perform a remote transfer of the encryption software, or of control parameters (not shown) to set particular characteristics of the encryption, from the Network Security Operations Center (NSOC) 110. In addition, as is known in the art, hardware keys (not shown) and other critical encryption data can be isolated within the crypto-engine 208 to prevent access by other devices (not shown) utilizing shared system resources.

The Fig. 2 block diagram depicts a DSP cluster 203 connected to the shared memory 209. The DSP cluster 103 performs data analysis , packet filter and other operations requiring high-speed computation, which the CPU 202 cannot perform at the required packet data rates, on packet data passed to the DSP cluster 209 from the media interfaces 206.

As can be seen in the detailed example SUNA 108 shown at Fig. 3, one preferred implementation of the DSP 203 is by multiple DSPs 203A, which are collectively arbitrated by a CPU subsystem 202A. The DSPs 203A share memory resources and are configured by the CPU subsystem 202A. Similar to the above-described crypto-engine 208, the software for the DSP cluster 203 are loaded either during manufacture, during installation, or by remote upload from the NSOC 110.

Local support of these DSP chips is well documented by their various manufacturers, and is implied by convention.

System integrity and operational monitoring of the SUNA 108 are provided by an ancillary processor 205, which also allows for redundant connectivity via ancillary media interface 204. The ancillary connection to the NSOC 110 is achieved via outboard calls initiated by the ancillary processor 205 directly to the NSOC 110 via Public Switched Telephone Network (not shown). Encryption and separate keyed security systems for the ancillary connection would also be used.

A more detailed example of the SUNA 108 unit technology is depicted at Fig. 3. The Fig. 3 system can be a stand-alone hardware unit or can be a PCI, or equivalent, plug-in for use in an existing system. In the Fig. 3 example a CPU 302 and an I/O processor 307, which are particular embodiments of the CPU 202 and I/O processor 207 of Fig. 2, are implemented by a single CPU chip labeled as 302A. An example chip 302A is a Motorola MPC 8260 or equivalent.

The Fig. 3 example embodiment utilizes multiple buses, with the bus labeled BUS 60x used for the cache memory 304, the main memory 309A, and the boot memory 306. The boot memory 306 may be a flash or ROM based device or other small non-volatile memory. A second bus, labeled PCI, is used for interface to mass storage devices 314, within the memory unit 309A, via the secondary interface 308 which, in the depicted example, is a PCI-to-IDE Bridge. The mass storage devices 314 in the Fig. 3 example include, for example, a hard disc drive and a CD-ROM (not numbered). The memory unit 309A also includes a solid state flash disk 312.

The Fig. 3 example SUNA 108 also contains PCI or equivalent expansion slots 314 and 316 for both custom and off-the-shelf expansion cards (not shown). The Fig. 3 example further includes a DSP cluster 303, which corresponds to the DSP unit 203 of Fig. 2. The DSP cluster 303 consists of multiple DSP chips 303A such, for example, ADSP-2189, and a crypto-engine 308, which corresponds to the crypto-engine 208 of the Fig. 2 general embodiment. An example hardware for the crypto-engine 308 is an ADSP 214L.

Interface for media, a real time clock (RTC) and diagnostic/installation are provided directly on the CPU subsystem 302A by the I/O communication processor 307. Ports P1 and P2 are provided for connection to an interface unit 206, corresponding to the same item on Fig. 2, having media controllers and interfaces 320 and 322. For the depicted example of Fig. 3 the interfaces 320 and 322 consist of a PM5348 transceiver and an LTX974A transceiver. The particular output, in terms of media and format, for each of the media transceivers 320 and 322 is determined by or configured for the particular end user. Connections for a real-time clock or RTC 324, a local configuration and monitoring port 326, and a stacking bus 328 are provided for by bus P3.

The ancillary processor 305 may, for example, be

Motorola MC68340. As shown in Fig. 3 the ancillary processor 305 is connected to the co-processor port COP of the CPU 302. However, as will be understood by one of ordinary skill in the art, other connection schemes between the CPU 302 and the ancillary processor 305 may be used. A standard "plain old telephone system", or POTS modem 330 implements what is shown as the ancillary media interface 204 of Fig. 2. The POTS modem is for purposes of example, as any valid network could be used as long as it provides redundancy and, if desired, enhanced security.

The Fig. 3 system further includes a power supply 332 and back-up batteries 334, in accordance with usual design practices.

Fig. 4 shows an optional embodiment of the present invention, which incorporates a SUNA 408 in accordance with the examples of Figs. 2 and 3, integrated into another's third-party telecommunication system 402. The integrated device 402 is termed, for purposes of this description, a SUNA Enabled Device or SED. Example SED 402s include a SUNA 108 incorporated into connectivity devices such as xDSL modems (not shown), cable modems (not shown), switches and routers (not shown). Advantages of the incorporated SED 402 include lower cost and transparency to the end user. As contemplated by this invention, the straightforward design, low size and weight of the SUNA 108 make the SUNA 108 equipped connectivity device 402 affordable enough to the end user such that the SUNA would be readily selected.

In the example SED 402 of Fig. 4, a SUNA core 408 is placed between a telecommunication provider's interface circuitry, referenced herein as TPIC 404, and a plurality of media interfaces 406 via an optional bypass control circuit 407, under the control of the TPIC 404. Connection of the TPIC 404 to the telecommunication provider specific media interface 403, as in a standard non SED device. An ancillary media interface 405, which corresponds to the interface 305 and 330 described in reference to Fig. 3, is connected to the SUNA core 408

Fig. 5 shows an example system similar to the system of Fig. 1, but having the SED device 402 of Fig. 4 in place of the separate SUNA 108 and connection device 104. All other functional blocks of Fig. 5 are identical to Fig.1 and, accordingly, are numbered the same. Referring to Fig. 5, connection to the customer network 100 as well as to the standalone user end point devices 102 affords the end user multiple secure ports to interface to the Internet. Connection to the ancillary network is shown separately, as would be the case in the POTS implementation of Fig. 3. Both the primary and ancillary connections are provided to the NSOC 110 for use in monitoring and maintaining the SED device.

Referring to Figs. 1 and 5, configuration of the SUNA 108, or the SED 402 is automatically performed after the connection to a service provider's demarcation point by virtue of the integration with a provider's installation procedure. The configuration consists of a simple notification sent manually at the time of install or, alternatively, could be fully incorporated into a service provider's interface boot-up sequence that occurs during installation.

An SED 402 or SUNA 108 would initiate a secure session, in accordance with session rules and methodologies well known to ones of skill in the art, with the NSOC 110, using any of the various encryption methods common to those previously referenced. A valid account found in an NSOC database would cause access of subscriber configuration data and files for the subscribed services. Subscriber services could include but are not limited to NSOC 110 and third party derived security and management algorithms, processes, keys and key techniques, intrusion detection and automated testing of firewalls using up-to-the-minute knowledge amassed at the NSOC 110. Subscription services can also be tiered, allowing for customer-specified levels of interaction of an SED 402 with that of the NSOC 110 including modification of the list of services provided. A tiered approach affords the ability of a telecommunication providers to offer services tailored for a customer depending on the sophistication of the customer's usage.

The operating system for the SED 402 or SUNA 108 is preferably a stable, robust, real-time operating system, having a wide installed base and having substantial third-party support, as well as large libraries of share-ware and freeware available. One example of such an operating system is OpenBSD.

After initial configuration, either periodically in response to new security information provided to the NSOC 110, the NSOC opens new sessions with one or more of the subscribing end-user's SUNA 108 and/or SED 402 connection devices, transfers new and updated security instructions to each. As a result, each of the updated end users' SUNA units 108 and SEDs 402 updates the filtering operations performed by the CPU 302 and DSP array 203 within each, as well as the encryption algorithms performed by their respective crypto-engines 308. This updating does not require action on the part of the end user's network system administrator. As a result, each subscribing end user immediately benefits from the updated information received by the NSOC 110, at minimal cost, without the current substantial risk of the local updating being incorrect, inadequate, or out of date. Further, the uniformity among the SUNA units 108 or the SED units 402, even over large number of end users, ensures that the updating received from the NSOC 110 will operate correctly, without the usual problems of integrating third party security measures into the particular hardware, and software systems, of each particular end-user.

While the foregoing invention has been described with specific references to examples of its preferred embodiments, it should be understood that various substitutions, variations, and modifications may be made thereto without departing from the scope of the invention as defined in the appended claims.

CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. A method for controlling traffic between a first and a second network comprising steps of:

connecting an interface unit between said first and second network, said interface unit having a processor and a data storage unit;

providing a management unit remote from said first network;

transferring an alarm criteria from said management unit to said interface unit;

storing said alarm criteria in said data storage unit;

receiving, at said interface unit, a digital communication between said first network and said second network;

comparing a content of said digital transmission to said alarm criteria, said comparing performed by said data processor; and

generating an alarm from said interface unit based on said comparing.

2. A method according to claim 1 further comprising a step of blocking said digital transmission from being communicated between said first network and said second

network based on said comparing.

3. A method according to claim 1 further comprising steps of:

providing an encryption unit with said interface unit, said encryption;

loading an encryption algorithm into said encryption unit; and

selectively encrypting digital communication from said first network to said second network, according to said encryption algorithm, based on a result of said comparing step.

4. A method according to claim 1 further comprising steps of

providing an encryption unit with said interface unit, said encryption;

loading an encryption algorithm into said encryption unit;

transmitting an encryption selection criteria from said remote management unit to said encryption unit; and

selectively encrypting a digital communication from said first network to said second network, according to said encryption algorithm, based on said encryption selection criteria.

Fig.1

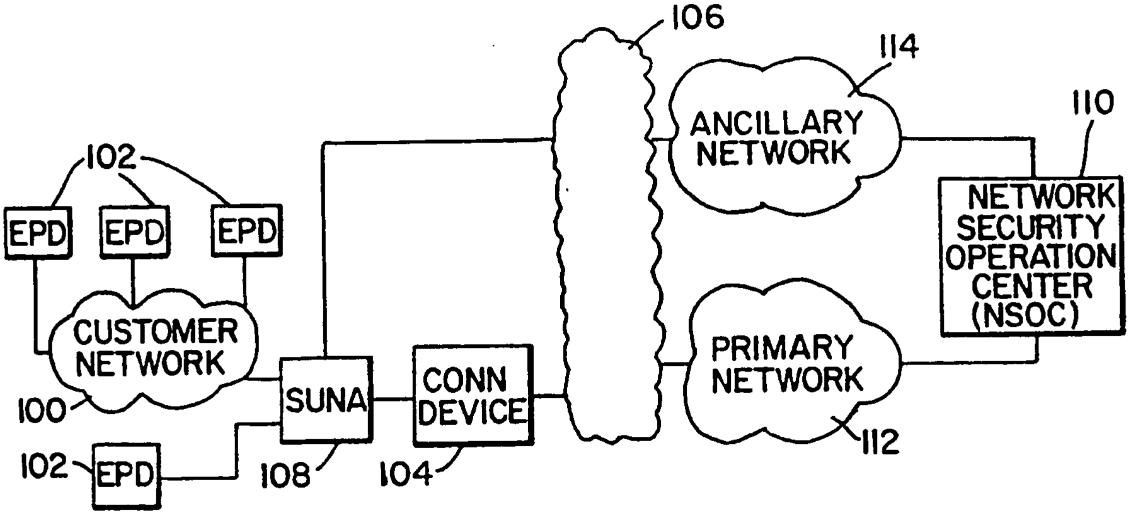

106
114
110
ANCILLARY NETWORK
102
EPD
EPD
EPD
NETWORK SECURITY OPERATION CENTER (NSOC)
CUSTOMER NETWORK
PRIMARY NETWORK
100
SUNA
CONN DEVICE
112
102
EPD
108
104

Fig.2

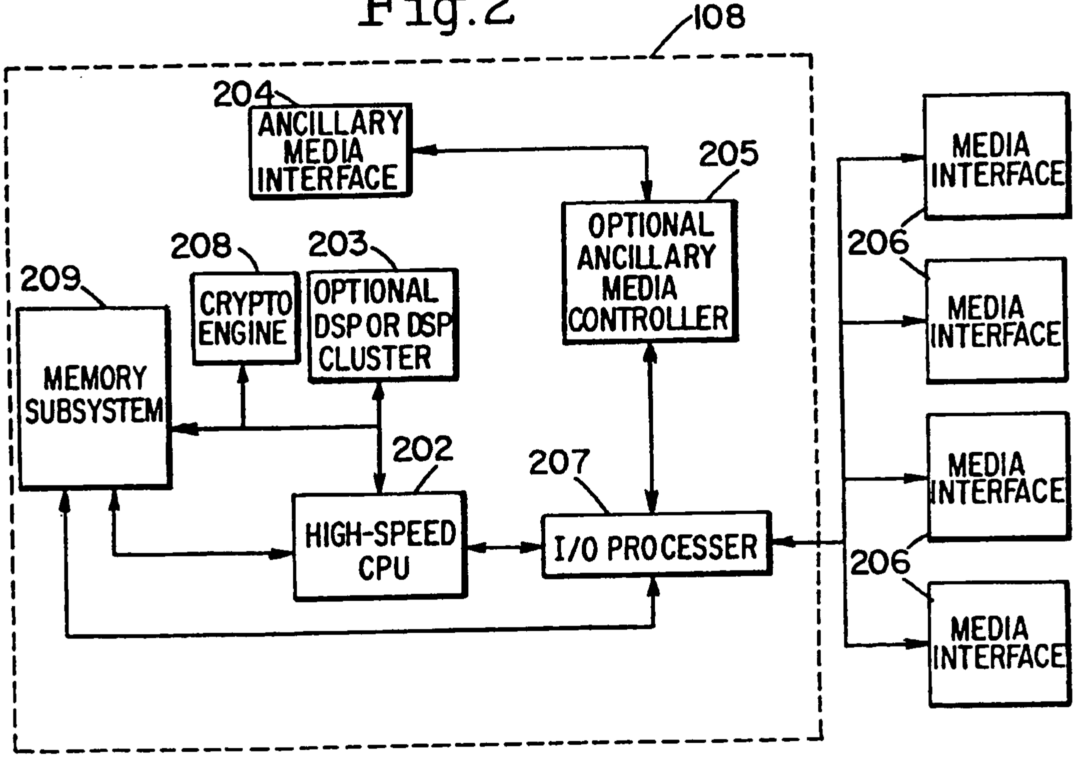

108
204
ANCILLARY MEDIA INTERFACE
205
OPTIONAL ANCILLARY MEDIA CONTROLLER
208
203
209
CRYPTO ENGINE
OPTIONAL DSP OR DSP CLUSTER
MEMORY SUBSYSTEM
202
207
HIGH-SPEED CPU
I/O PROCESSER
MEDIA INTERFACE
206
MEDIA INTERFACE
MEDIA INTERFACE
206
MEDIA INTERFACE

Fig. 3 2/3

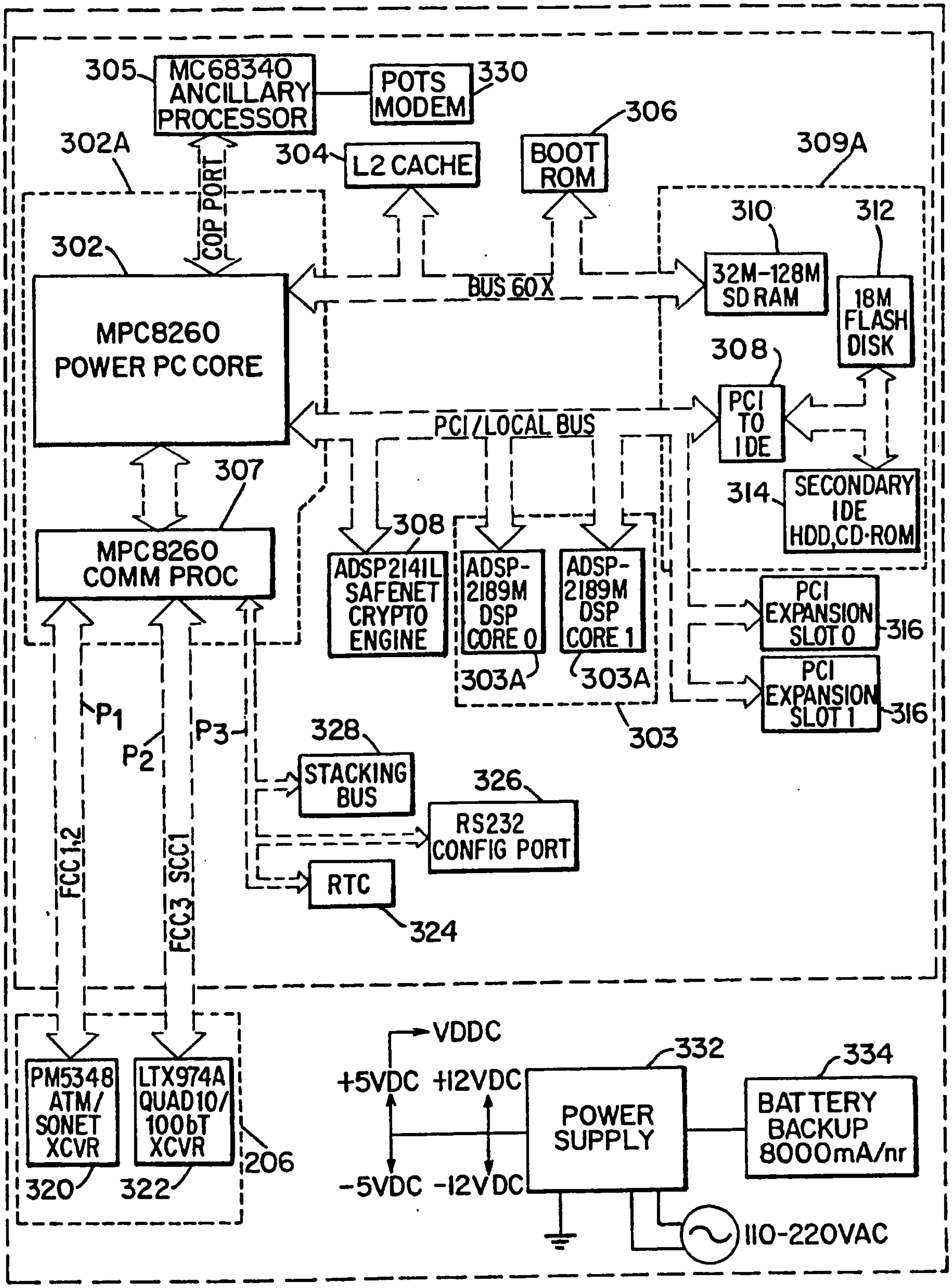

305
MC68340 ANCILLARY PROCESSOR
POTS MODEM
330
302A
304
L2 CACHE
BOOT ROM
306
309A
COP PORT
302
310
312
32M-128M SD RAM
BUS 60X
18M FLASH DISK
MPC8260 POWER PC CORE
308
PCI TO IDE
PCI/LOCAL BUS
307
314
SECONDARY IDE HDD,CD-ROM
308
MPC8260 COMM PROC
ADSP2141L SAFENET CRYPTO ENGINE
ADSP-2189M DSP CORE 0
ADSP-2189M DSP CORE 1
PCI EXPANSION SLOT 0
316
PCI EXPANSION SLOT 1
316
303A
303A
P1
P2
P3
303
328
STACKING BUS
326
RS232 CONFIG PORT
RTC
324
FCC1,2
FCC3 SCC1
VDDC
332
334
+5VDC
+12VDC
POWER SUPPLY
BATTERY BACKUP 8000mA/nr
PM5348 ATM/ SONET XCVR
LTX974A QUAD10/ 100bT XCVR
206
320
322
-5VDC
-12VDC
110-220VAC

Fig.4

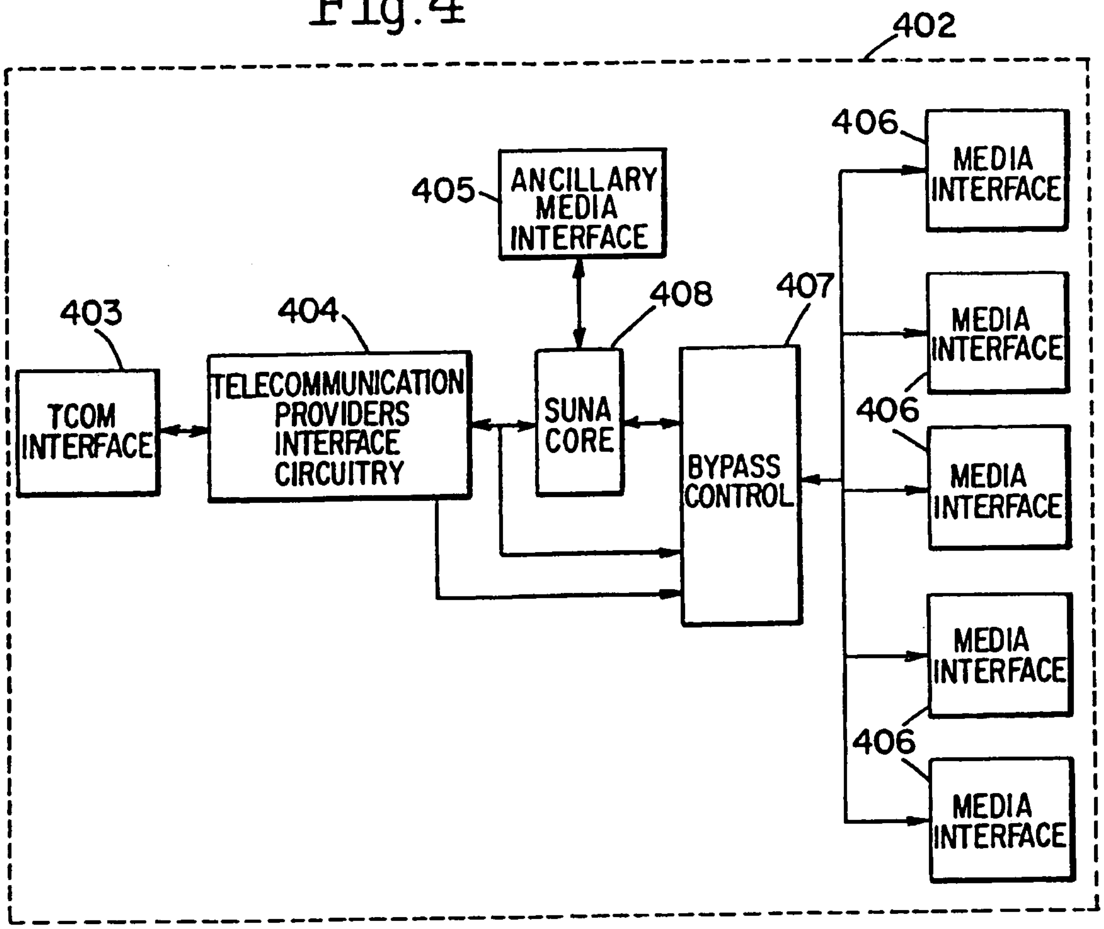
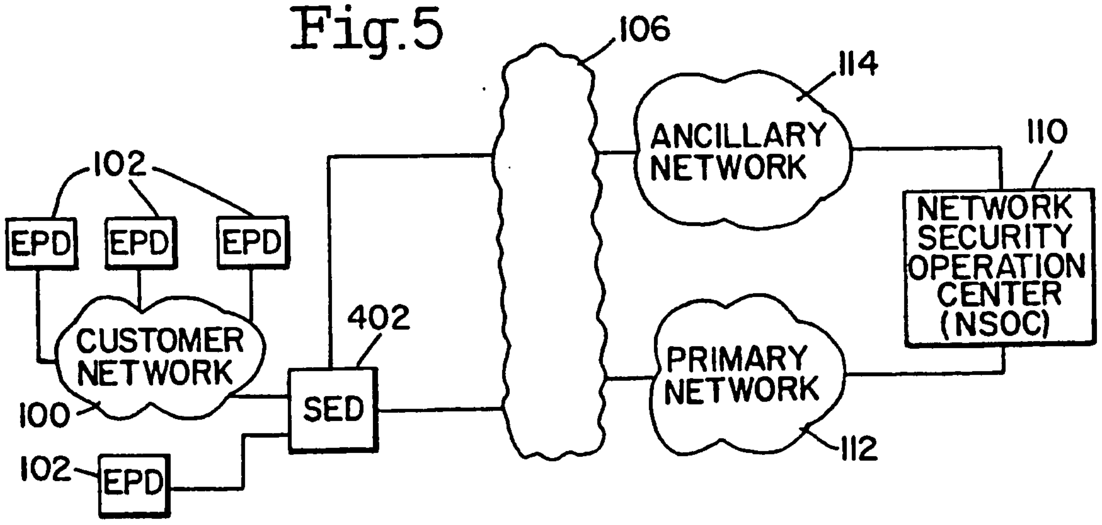

402
403
TCOM INTERFACE
404
TELECOMMUNICATION PROVIDERS INTERFACE CIRCUITRY
405
ANCILLARY MEDIA INTERFACE
408
SUNA CORE
407
BYPASS CONTROL
406
MEDIA INTERFACE
MEDIA INTERFACE
406
MEDIA INTERFACE
MEDIA INTERFACE
406
MEDIA INTERFACE

Fig.5


106
114
ANCILLARY NETWORK
110
NETWORK SECURITY OPERATION CENTER (NSOC)
102
EPD
EPD
EPD
CUSTOMER NETWORK
100
402
SED
PRIMARY NETWORK
112
102
EPD

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/14279

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 15/177
US CL : 713/1
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/1, 200,201; 709/223,235,249,250

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

East, West
searched terms: telephone network and router, lan, router, comparing, mapping.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,737,333 A (CIVANLAR ET AL) 07 APRIL 1998, ALL	1-4
Y	US 5,586,260 A (HU) 17 DECEMBER 1996, col.6 lines 12-29	1-4
Y,P	US 5,930,359 A (KEMPKE ET AL) 27 JULY 1999. col.9 lines 32-45 and figure 7	3-4

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 08 AUGUST 2000	Date of mailing of the international search report 22 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Lee, Thomas Eugenia Logan Telephone No. (703) 308-7024